UNIVERSIDADE ESTADUAL DE CAMPINAS
FACULDADE DE TECNOLOGIA

JULIANA ALMEIDA MORRONI

PROPOSTA DE ARQUITETURA DE SEGURANÇA PARA O SISTEMA HESTIA

Baseado no projeto de iniciação tecnológica: Segurança da Informação para um Sistema de Anamnese Neurológica Infantil (Hestia)

LIMEIRA - SP

2021

Sumário

Resumo **1**

1. Introdução **2**

2. O que deve ser feito **3**

3. Legislações **3**

3.1 Lei Geral de Proteção de Dados - LGPD 3

3.2 Gerenciamento Eletrônico de Documentos - GED 6

3.3 Conselho Federal de Medicina (CFM) e a Sociedade Brasileira de Informática em Saúde (SBIS) 7

3.4 Legislações Eletivas 7

4. Proposta para o Sistema **10**

5. Proposta para a Rede **11**

6. Políticas de Segurança **14**

6.1. Permissões 17

6.2 Regras de senha segura 17

6.3 Auditoria 17

6.4 Responsabilidades da área de TI 17

6.5 Política de treinamento aos colaboradores 18

7. Proposta para o Banco de Dados **18**

7.1 Criptografia 18

7.2 Controle de Acesso 20

7.3 Backup 21

8. Conclusões **22**

9. Referências **22**

Resumo

Nesta proposta são retratados quais serão as definições de uma arquitetura de segurança para ser aplicada no sistema Hestia, de forma a atender as diretrizes de segurança de sistemas médicos, em especial às Resoluções CFM 1.821/2007, 2.227/2018 e 2.056/2013 do Conselho Federal de Medicina, à norma ABNT NBR ISO/IEC 27002:2013, à Lei Geral de Proteção de Dados (LGPD) e à *Health Insurance Portability and Accountability Act* (HIPAA – Lei de portabilidade e responsabilidade de provedores de saúde) (USA).

O Hestia é um software criado para anamnese em deficiências sensoriais, voltada à neurologia infantil. A anamnese é definida como a 1ª entrevista realizada pelo profissional de saúde ao seu paciente. Nela, o profissional da saúde consegue obter as informações iniciais necessárias para obter uma melhor perspectiva do assunto. Este trabalho consiste em avaliar e recomendar as maneiras de manter e garantir a privacidade e segurança dos dados pessoais subsequentes da anamnese e assim traçando os próximos passos para programadores aplicarem ao sistema.

1. Introdução

Muitos sistemas de informação e redes de computadores são expostos a diversos tipos de ameaça à segurança de seus dados. Danos que podem ser causados por diversos fatores, incluindo danos causados por códigos maliciosos, *hackers* e ataques de *denial of service* que estão se tornando cada vez mais frequentes e mais sofisticados.

A questão da segurança da informação remete ao fato de que os dados são importantes e possuem determinado valor, e quando há valor devemos assegurar sua segurança. A informação, hoje em dia, é um ativo que, como qualquer outro ativo importante, é essencial para estes sistemas e necessita ser adequadamente protegida. O conceito importante é evitar ou reduzir os riscos de vazamento e garantir o controle do acesso a estes dados.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por procedimentos apropriados à arquitetura do sistema que será utilizado. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes.

Nesta pesquisa são abordados requisitos de segurança de informação necessários para proporcionar a segurança dos dados manipulados no sistema Hestia, com o intuito de definir uma arquitetura de segurança de TI. A base de seu desenvolvimento será uma nova proposta/versão para a ferramenta Hestia, cujo sistema é tecnicamente antigo e precisa de atualizações.

O Hestia está em sua terceira versão e tem distribuição gratuita. Opera em rede, em arquitetura cliente/servidor, o que significa que pode gerenciar recursos comuns aos usuários, como por exemplo um banco de dados centralizado, evitando problemas de redundância. Pode ainda, realizar mudanças que não afetarão o sistema, como substituir, reparar e atualizar informações.

A ferramenta será utilizada em larga escala e sem limitações, disponível para seu uso na Faculdade de Ciências Médicas da Unicamp, por isso a necessidade de uma arquitetura de segurança se torna mais relevante e pertinente, pois dados e informações estarão na Internet. Dados estes considerados sensíveis, que pela sua própria natureza podem levar o seu titular a vivenciar práticas discriminatórias, tais como dados sobre a origem racial ou étnica, referentes à saúde ou à vida sexual; ou permitir a sua identificação de forma inequívoca e persistente. Portanto, devem ser tratados de forma diferenciada, com camadas de segurança adicionais e com bases legais distintas.

Tecnicamente na época em que a ferramenta foi criada, não era necessário um sistema de segurança, pois não existia um risco proeminente por não haver tanto acesso à informação como há hoje em dia. Com o temor de possíveis ataques cibernéticos, a prática de proteção à segurança da

informação se tornou indispensável no sistema Hestia. Para isso, serão utilizados artigos científicos, normas e resoluções do Conselho Federal de Medicina, tais como Resoluções CFM 1.821/2007, 2.227/2018 e 2.056/2013, Lei Geral de Proteção de Dados (LGPD), que informam como estes dados devem ser tratados perante a Lei.

Serão mencionados recursos, procedimentos e recomendações necessárias para atingir os padrões de seguranças propostos para preservar dados em repouso com criptografia de banco de dados, com sugestões de proteção física ao servidor, assim como um inventário com tópicos importantes ao programador/arquiteto para serem cumpridos e executados da melhor maneira.

Deste modo, tal abordagem deverá ser específica e muito bem detalhada para cobrir todas as dimensões que possam surgir, sejam princípios de desriminação, vazamento de dados, não adequação aos princípios das normas e assim por diante. Ela deve atender aos requisitos de sistemas médicos que sejam imprescindíveis, estando em comum acordo com as normas e resoluções relacionadas ao meio da segurança, as quais devem ser desenvolvidas pelo programador seguindo o modelo proposto.

2. O que deve ser feito

O resultado esperado é trazer uma proposta de arquitetura para a segurança dos dados sensíveis utilizados pela ferramenta Hestia, para tentar garantir e assegurar o controle de acesso aos dados manuseados pelos usuários que neste caso serão: o médico da Faculdade de Ciências Médicas e possíveis pesquisadores que necessitarem das informações contidas no sistema.

O programador deverá seguir os passos da proposta de arquitetura representada, se atentando aos requisitos pertinentes à segurança da informação descritos no tópico seguinte. Seguidamente do cumprimento das 3 propostas aqui desenvolvidas: Proposta para o Sistema, Proposta para a Rede e a Proposta para o Banco de Dados.

3. Legislações

O sistema Hestia usa dados pessoais que devem ser protegidos por legislações e normas de segurança e o compartilhamento de tais informações é restrito. Por outro lado, são absolutamente necessários para o atendimento do paciente e para pesquisa médica.

Então devemos destacar aqui que os dados devem ser protegidos em seu armazenamento, transferência e consulta e também precisam ser vistos por pessoas de direito. Com base no estudo feito, o sistema deve atender às seguintes Legislações para cumprir tais requisitos:

3.1 Lei Geral de Proteção de Dados - LGPD

Estar em conformidade com a Lei Geral de Proteção de Dados significa estar em adequação à proteção do uso de informações pessoais, de sua privacidade, transparência, coleta adequada, armazenamento e compartilhamento dos dados dos usuários.

A lei elenca dez princípios que as organizações devem obedecer quanto ao tratamento de dados. A pesquisa feita para a proposta do Hestia leva em destaque os princípios da finalidade, da adequação, da necessidade, da transparência e da não discriminação, apesar disso, o programador deve garantir que todos sejam cumpridos. As descrições de cada princípio, juntamente das ações a serem realizadas pelo programador estão dispostas a seguir:

1- Finalidade

O que diz a lei:

Este princípio determina que não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas**.** É necessário possuir uma finalidade específica, informada ao titular. O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados. Essas finalidades também devem estar dentro dos limites da lei e devem vir expressamente acompanhadas de todas as informações relevantes para o titular.

Para o programador:

Quando o usuário abrir o formulário, o médico ou atendente deverá ser lembrado de informar ao titular dos dados ou responsável, a finalidade dos dados solicitados. Garantir e demonstrar a adequação dos dados (médicos, sociais, etimológicos, etc), que são pertinentes ao diagnóstico ou identificação.

2- Adequação

O que diz a lei:

Os dados pessoais tratados devem ser compatíveis com a finalidade informada. Ou seja, a justificativa deve fazer sentido com o caráter da informação que se pede.

Para o programador:

O sistema já pede esse tratamento.

3- Necessidade

O que diz a lei:

A coleta e utilização de dados pessoais deve se restringir ao mínimo necessário para a realização das finalidades pretendidas. Quanto mais dados tratados, maior será a responsabilidade, inclusive em casos de vazamentos e incidentes de segurança.

Para o programador:

Não existe “declaração sobre colunas” a ser feita pelo programador.

4- Transparência

O que diz a lei:

Garantia, aos titulares, de informações claras e precisas sobre o uso de seus dados pessoais. Todas as informações passadas, em todos os seus meios de comunicação, devem ser verdadeiras e fiéis.

Para o programador:

Garantir ao titular quais dados são utilizados e como serão usados, durante o acompanhamento do paciente. Podendo destacar ao usuário que esta ação é necessária. De preferência conter um formulário de informação ou consentimento impresso. Além disso, não poderão ser compartilhados os dados pessoais com outras pessoas de forma oculta. Se for preciso repassar estes dados para terceiros, o titular precisará saber.

5- Não discriminação

O que diz a lei:

Impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos. Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares. A LGPD criou regras específicas para o tratamento de dados que frequentemente são utilizados para discriminação, os chamados dados pessoais sensíveis, como os que tratam sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual e dado genético ou biométrico.

Para o programador:

Reforçar mecanismos de controle de acesso para permitir apenas usuários legítimos. Além de incluir informações no formulário de consentimento do paciente sobre este princípio de não descriminação.

6- Princípio do livre acesso

O que diz a lei:

Os titulares dos dados têm a garantia de consulta sobre a forma e a duração do armazenamento de seus dados pessoais, bem como sobre sua integralidade. Terá o direito de consultar, de forma simples e gratuita, todos os dados que o sistema detenha a seu respeito.

Para o programador:

Garantir único acesso ao médico e ao pesquisador à estas informações sensíveis, as quais estejam em formato anônimo. Incluir estas informações no formulário de consentimento.

7- Princípio da qualidade dos dados

O que diz a lei:

Esse princípio assegura aos titulares dos dados, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Para o programador:

Deverá ter mecanismos de registro e correção dos dados. Como edição, exclusão e atualização do banco de dados.

8- Princípio da segurança

O que diz a lei:

Deverão utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dos dados pessoais de suas bases.

Para o programador:

Proteger dados de acesso não autorizados, controle de acesso ao sistema, o banco de dados tem que ser acessível apenas por uma máquina segura. Utilizar criptografia no banco de dados em repouso e em sua transmissão.

9- Princípio da prevenção

O que diz a lei:

Sejam adotadas as medidas necessárias para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. É um dos pilares da Segurança da Informação.

Para o programador:

Buscar a antecipação de eventualidades, com a adoção de medidas para prevenir a ocorrência de danos em razão do tratamento de dados pessoais.

10- Princípio da responsabilização e da prestação de contas

O que diz a lei:

Espera-se que o controlador ou o operador demonstrem todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas. Além de se preocuparem em cumprir integralmente a Lei, devem ter provas e evidências de todas as medidas adotadas, para demonstrarem a sua boa-fé e a sua diligência.

Para o programador:

Detalhar a arquitetura de segurança do sistema. Comprovar que foi realizado treinamento na equipe que utiliza o sistema (se foi necessário), garantir a utilização de protocolos e sistemas que garantam a segurança dos dados e o acesso facilitado do titular sempre que preciso.

3.2 Gerenciamento Eletrônico de Documentos - GED

O Gerenciamento Eletrônico de Documentos (GED) permite que as empresas automatizem seus processos por meio da digitalização de documentos, para que o gerenciamento seja feito de forma integrada. Além disso, permite que os usuários acessem as informações e documentos, previamente digitalizados, de forma ágil e segura, podendo ser feito de forma remota, de qualquer hora e lugar.

Este processo de digitalização de documentos foi sancionado pela a Lei nº 13.787, que regulamenta a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuários de pacientes. Esta lei se junta à Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a Proteção de Dados Pessoais e que tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade.

À vista disso, o programador deve garantir a utilização da tecnologia GED para automatizar os processos hospitalares, fazendo com que o Hestia garanta o cumprimento das obrigações exigidas na lei quanto ao manuseio, arquivamento e descarte desses documentos. Trazendo tais benefícios:

- Facilidade na busca por documentos;
- Armazenamento dos arquivos em Nuvem, o que possibilita redução de espaço físico e em HD, o que permite o seu acesso de qualquer lugar;
- Solução personalizada para cada necessidade;

- Redução de tempo desperdiçado e custos com documentos;
- Segurança nas informações com auditoria de todas as ações de cada usuário;
- Cópias de segurança e backup periódico;
- Baixo risco de extravio e perda de prontuários e históricos;
- Garantia de confidencialidade.

O GED é composto por diversas ferramentas, as necessárias para o sistema Hestia estão listadas a seguir:

- DI: com o Processamento de Imagens para Documento (DI), o scanner consegue identificar, armazenar e visualizar as imagens de um documento, caso haja necessidade durante a anamnese como inclusão de algum documento ou resultados de exames, tornando-os digitais por meio de um mapa de bits.
- RM: o sistema também permite o Gerenciamento de Registros ou Gerenciamento de Documentos (Document Management), que faz a gestão a longo prazo dos documentos físicos e digitais, controlando seu ciclo de vida, desde a criação até arquivamento permanente ou exclusão.
- COLD/ERM: com o Enterprise Report Management é possível fazer a formatação, indexação e compactação de relatórios, inventários, faturas e outros conteúdos, permitindo a liberação de espaço e facilitando a busca por informações.

De maneira geral, o programador deverá seguir os protocolos e utilizar as ferramentas elencadas para garantir que todos os arquivos poderão ser organizados por meio digital pelo GED. Desta forma, eles ficam disponíveis para consulta a qualquer momento e facilmente acessados. Os documentos podem estar em diversos formatos, podendo ser administrados de melhor forma, o que contribui para uma maior fluidez no desenvolvimento de atividades em tempo real.

3.3 Conselho Federal de Medicina (CFM) e a Sociedade Brasileira de Informática em Saúde (SBIS)

Estabelece que o Conselho Federal de Medicina (CFM) e a Sociedade Brasileira de Informática em Saúde (SBIS), mediante convênio específico, expedirão selo de qualidade dos sistemas informatizados que estejam de acordo com o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, aprovado na resolução nº1.821/2007.

3.4 Legislações Eletivas

Com base no estudo feito, todos os dados utilizados pelo Hestia possuem caráter pessoal e portanto diante das várias normas existentes citadas aqui é importante garantir que este sistema mantenha a privacidade de todas as informações criadas ou recebidas de pacientes. A seguir, normas e legislações consideradas importantes, porém seu uso não é obrigatório:

3.4.1 HIPAA (Lei norte americana de Portabilidade e Responsabilidade de Seguros de Saúde)

Todas as pessoas têm direito à confidencialidade, exceto se concederam permissão para divulgação. Uma lei federal dos EUA, a Lei da Portabilidade e Responsabilização do Seguro de Saúde (Health Insurance Portability and Accountability Act, HIPAA – (privacidade das informações de saúde)) se aplica à maioria dos profissionais da área de saúde, e sua regulamentação, conhecida como Regras de Privacidade (Privacy Rule), define regras detalhadas em relação à privacidade, acesso e revelação das informações. Por exemplo, a HIPAA especifica o seguinte:

- As pessoas devem ser normalmente capazes de ver e obter cópias de seus registros médicos e solicitar correções, se encontrarem erros;
- Qualquer pessoa legalmente autorizada a tomar decisões de saúde para uma pessoa incapacitada tem o mesmo direito de acesso às informações médicas pessoais dela;
- Os profissionais da área da saúde devem rotineiramente divulgar suas práticas em relação à privacidade das informações médicas pessoais;
- Os profissionais da área da saúde podem compartilhar as informações médicas das pessoas, mas apenas entre eles e apenas o necessário para fornecer o tratamento médico;
- As informações médicas não podem ser divulgadas para fins de mercado;
- Os profissionais da área da saúde devem tomar as medidas razoáveis para garantir que suas comunicações com a pessoa sejam confidenciais;
- As pessoas podem consultar o arquivo sobre as práticas de privacidade dos profissionais da área da saúde (diretamente com o profissional de saúde ou no Escritório de Direitos Civis no Departamento de Serviços de Saúde e Humanos dos EUA).

3.4.2 NBR ISO/IEC 27002:2013

Encontram-se diversas metodologias e práticas em segurança da informação que são bem conhecidas na área. Entre elas estão *CobiT, ITIL* e a *ABNT NBR ISO/IEC 27002*, essas são exemplos de normas que padronizam o modelo de como uma organização deve estruturar sua gestão da segurança da informação.

Esta pesquisa foca na norma que estrutura um código de boas práticas para que organizações consigam cuidar de seus dados e evitar o vazamento de informações relevantes. São algumas das atividades da NBR ISO/IEC 27002:2013 – Políticas para segurança da informação que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse.

As vantagens proporcionadas pela série de normas da ISO 27002 são representativas para as empresas, principalmente pelo fato de serem reconhecidas mundialmente. Seguem alguns benefícios associados a aplicação da norma:

- Melhor conscientização sobre a segurança da informação;
- Maior controle de ativos e informações sensíveis;
- Oferece uma abordagem para implantação de políticas de controles;
- Oportunidade de identificar e corrigir pontos fracos;
- Redução do risco de responsabilidade pela não implementação de um Sistema de Gestão de Segurança da Informação - **SGSI** (ferramenta corporativa para abordagem organizacional da questão). Ou determinação de políticas e procedimentos;
- Torna-se um diferencial competitivo para a conquista de clientes que valorizam a certificação;
- Melhor organização com processos e mecanismos bem desenhados e geridos;

- Promove redução de custos com a prevenção de incidentes de segurança da informação;
- Conformidade com a legislação e outras regulamentações.

Para (SÊMOLA, 2014), "A norma representa uma trilha que orienta as empresas dispostas a se estruturarem para gerir os riscos de segurança da informação". Sendo assim, é correto afirmar que a norma é apenas uma orientação, a organização que terá que buscar os meios para se adequar às diretrizes impostas na norma.

A parte principal da norma se encontra distribuída nas seguintes seções, que correspondem a controles de segurança da informação. As quais são aconselhadas que se siga:

Seção 5 – Política de Segurança da Informação

Deve ser criado um documento sobre a política de segurança da informação da empresa/instituição, que deve conter os conceitos de segurança da informação, uma estrutura para estabelecer os objetivos e as formas de controle, assim como, o comprometimento com a política estipulada.

Seção 6 – Organização da Segurança da Informação

Para implementar a Segurança da Informação em uma empresa/instituição, é necessário estabelecer uma estrutura para gerenciá-la da maneira adequada. Para isso, as atividades de segurança da informação devem ser coordenadas por representantes da organização, que devem ter responsabilidades bem definidas e proteger as informações de caráter sigiloso.

Seção 7 – Gestão de ativos

Ativo, segundo a norma, é qualquer coisa que tenha valor para a organização e que precisa ser protegido. Mas para isso, os ativos devem ser identificados e classificados, de tal forma que um inventário possa ser estruturado e posteriormente mantido. Além disso, eles devem seguir regras documentadas, que definem qual tipo de uso é permitido fazer com esses ativos.

Seção 8 – Segurança em recursos humanos

Antes de realizar a contratação de um funcionário/médico/pesquisador é importante que ele seja devidamente analisado, principalmente se for lidar com informações de caráter sigiloso. A intenção desta seção é mitigar o risco de roubo, fraude ou mau uso dos recursos. E quando o funcionário/médico/pesquisador estiver trabalhando, deverá estar ciente das ameaças relativas à segurança da informação, bem como de suas responsabilidades e obrigações.

Seção 9 – Segurança física e do ambiente

Os equipamentos e instalações de processamento de informação críticas ou sensíveis devem ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Seção 10 – Segurança das operações e comunicações

É importante que estejam definidos os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações. Isso inclui o gerenciamento de serviços terceirizados, o planejamento dos recursos dos sistemas para minimizar o risco de falhas, a

criação de procedimentos para a geração de cópias de segurança e sua recuperação e a administração segura de redes de comunicações.

Seção 11 – Controle de acesso

O acesso à informação, assim como aos recursos de processamento das informações e aos processos de negócios, deve ser controlado com base nos requisitos de negócio e na segurança da informação. Deve ser assegurado o acesso de usuário autorizado e prevenir o acesso não autorizado a sistemas de informação, a fim de evitar danos a documentos e recursos de processamento da informação que estejam ao alcance de qualquer um.

Seção 12 – Aquisição, desenvolvimento e manutenção de sistemas

Os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, autenticidade ou integridade por meios criptográficos.

Seção 13 – Gestão de incidentes de segurança da informação

Procedimentos formais de registro e escalonamento devem ser estabelecidos, e os usuários do sistema devem estar conscientes sobre os procedimentos para notificação dos eventos de segurança da informação, para assegurar que eles sejam comunicados o mais rápido possível e corrigidos em tempo hábil.

Seção 15 – Conformidade

É importante evitar a violação de qualquer lei criminal ou civil, garantindo estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

Seguir os princípios da certificação ISO/IEC 27002 é um passo altamente relevante, para garantir a segurança da informação de um sistema. Neste sentido, é primordial ressaltar a importância de as empresas possuírem profissionais certificados em seus times de segurança, dando maior apoio ao processo de implantação das boas práticas relacionadas à norma, bem como a obtenção de certificação corporativa ISO 27001.

E o mais importante é que tenha uma continuidade no programa, onde o mesmo tem que ser atualizado de acordo com as mudanças tecnológicas e de segurança. A avaliação por parte dos colaboradores é uma excelente alternativa para conseguir a média do nível de esclarecimento sobre segurança e assim criar um plano de reforço de acordo com a necessidade.

Alguns pontos devem ser levados em considerações são:

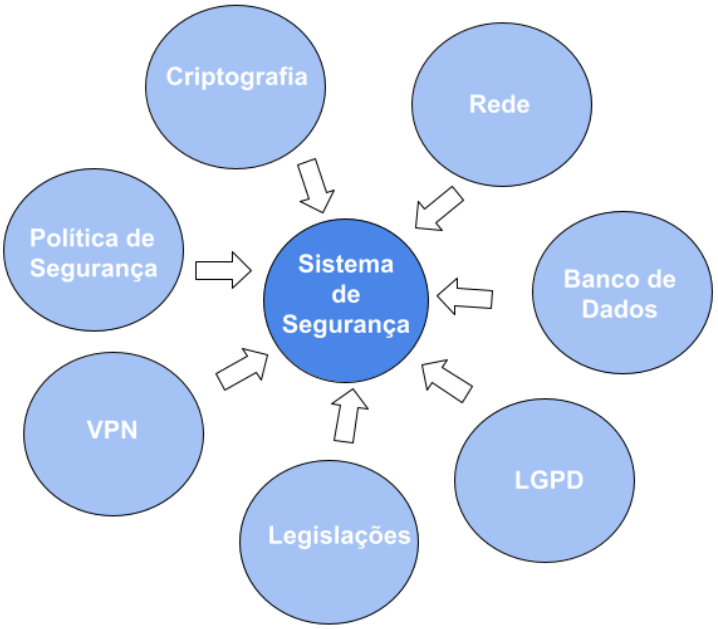
- A padronização dos processos e instruções de trabalho;
- Aplicar tecnologias capazes de garantir a segurança;
- Repassar formalmente as responsabilidades e as devidas penalidades;
- A classificação das informações;
- Ter treinamentos e informativos frequentemente.

4. Proposta para o Sistema

Será proposto um sistema que seja seguro o suficiente e atenda às normas e legislações aqui elencadas relacionadas à proteção de dados sensíveis, que também tenha uma política de segurança associada e um nível de atendimento da LGPD.

A proposta também requer elementos como criptografia de banco de dados, políticas de segurança e VPN, assim como exemplificado na Figura 1. Desta maneira, pode ser implementado um sistema completo em relação à segurança de seus dados, ou seja, que atenda todas as necessidades da organização e que esteja dentro das diretrizes de segurança da informação citadas até o momento.

Figura 1: Sistema proposto e seus elementos envolvidos



Fonte: Juliana Almeida Morroni (2021)

Como preferência a integração de uma interface gráfica é exigida, por tal motivo, o Hestia já apresenta Graphical User Interface (GUI), uma interface gráfica do usuário que permite a interação com os dispositivos digitais através de elementos gráficos. Embora não seja previsto inicialmente, o sistema poderá ter uma versão mobile, porém não é considerada essencial ao sistema proposto.

5. Proposta para a Rede

Para os propósitos deste trabalho, é necessário que se definam os principais conceitos, serviços e tecnologias em segurança de redes. A fim de estruturar as diversas tecnologias e homogeneizar os serviços de segurança da informação.

De acordo com (STALLINGS, 1999), qualquer metodologia ou abordagem adotada em uma organização/sistema deve considerar três aspectos de segurança da informação:

- ***Ataques de segurança:*** quaisquer ações que possam comprometer a disponibilidade, integridade, sigilo e autenticidade de uma informação pertencente a uma organização;
- ***Mecanismos de segurança:*** mecanismos projetados para se destacar, prevenir ou se recuperar de um ataque de segurança;
- ***Serviços de Segurança:*** funções que aumentam o nível de segurança dos sistemas de processamento de dados e das transmissões de informação em uma organização. Estes serviços podem usar um ou mais mecanismos de segurança.

Para tornar as redes mais seguras e confiáveis, deve-se estar atento às principais ameaças que podem comprometer e prejudicar os conceitos de integridade, privacidade e autenticidade das informações ali utilizadas. Estas ameaças podem ter origem interna ou externa, e é sabendo sua origem que podem ser definidos quais métodos de segurança serão mais assertivos.

Algumas possíveis formas de ataque:

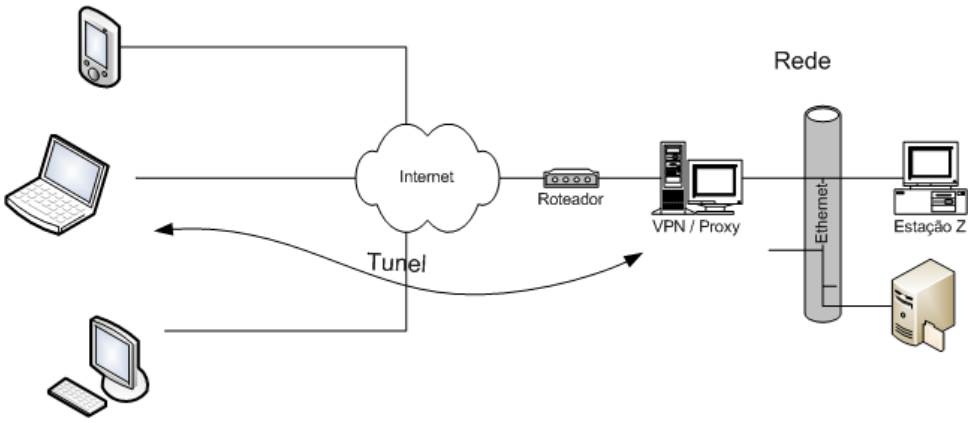
- **Ataque de Interrupção:** visa destruir ou interromper o serviço oferecido, ou seja, ataca-se a disponibilidade das informações;
- **Ataque de Interceptação:** tem como objetivo capturar o que está sendo transmitido sem que o sistema perceba, ou seja, ataca-se a privacidade das informações;
- **Ataque de Modificação:** é quando existe alteração da informação que está sendo transmitida, ou seja, ataca-se a integridade da mesma;
- **Ataque de Fabricação:** o atacante tem como finalidade se passar por um usuário do sistema, a fim de obter informações para transmitir dados na rede, ou seja, ataca-se a autenticidade das informações;
- **Ataques Ativos e Passivos:** Passivos, onde o sistema continua a operação sem a percepção de ter um invasor na rede e acontece roubo de informações; Ativos, onde o invasor prejudicá o sistema, atingindo os dados ou degradando os serviços, envolvendo modificações nos dados.

É necessário que se entenda que nenhum componente único pode garantir total segurança que seja 100% adequada, pois existem diversos casos e portanto deve-se manter uma atenção a estes pontos e usar recursos de segurança da informação adaptáveis a qualquer situação de ataques.

Por tal motivo, este estudo propõe a utilização de uma Rede Virtual Privada (VPN), sendo assim, uma rede virtual privada. Como Basta (2014, p 173) afirma “funciona basicamente criando uma rede de comunicações entre computadores e outros dispositivos que possuem acesso restrito a quem possui as credenciais necessárias”. Assim como a ferramenta Hestia que busca na base de dados (Interbase) os dados necessários para realizar a devida pesquisa.

A passagem de dados sensíveis pela Internet somente se torna possível com o uso de alguma tecnologia que torne esse meio altamente inseguro em um meio confiável. Com essa abordagem, o uso de VPN sobre a Internet parece ser uma alternativa viável e adequada.

Figura 2: Representação de uma Rede Virtual (VPN)

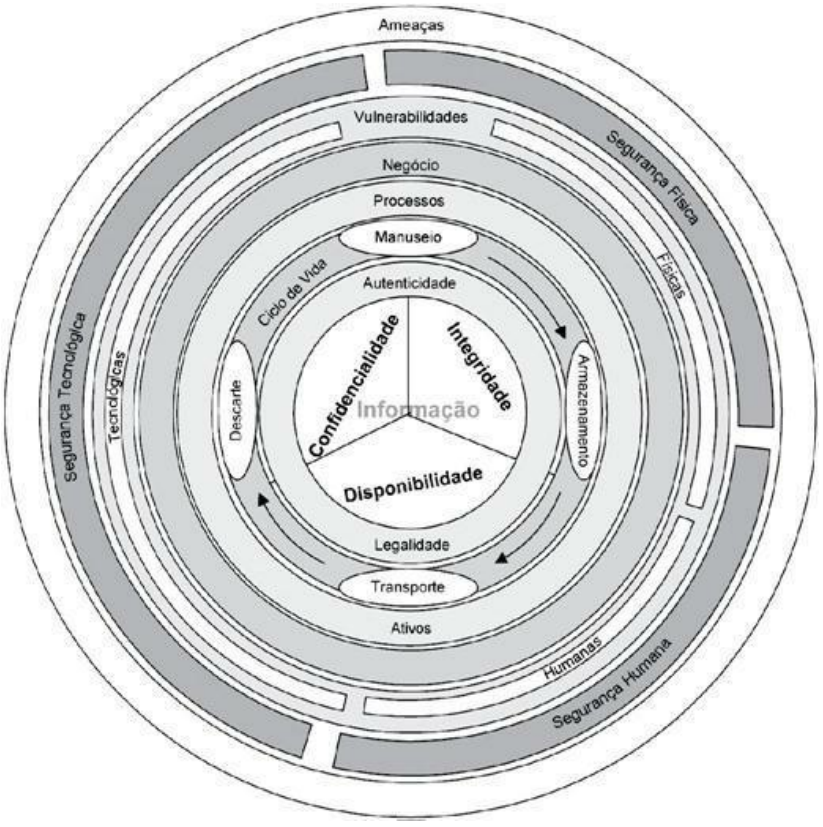


Fonte: Devmedia.com

Junto a isso, um modelo de Defesa em Profundidade também é proposto para fins adicionais à segurança. Pois uma camada única de segurança pode não ser eficaz diante da evolução rápida e inteligente dos crimes cibernéticos. A estratégia de defesa em profundidade constrói uma rede mais segura com a implementação de camadas e até a duplicação de certos métodos de proteção para minimizar a probabilidade de vazamentos.

Segundo (SÊMOLA, 2014), "São agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades". Essas vulnerabilidades podem ser físicas, naturais, de hardwares, e softwares, de comunicação e humanas. Há um grande risco de uma determinada ameaça utilizar dessas vulnerabilidades para realizar um ataque à segurança da informação, o que impossibilitaria a continuidade do negócio. O impacto gerado por um incidente na segurança, por ser analisado na Figura 3:

Figura 3 - Visão condensada dos desafios



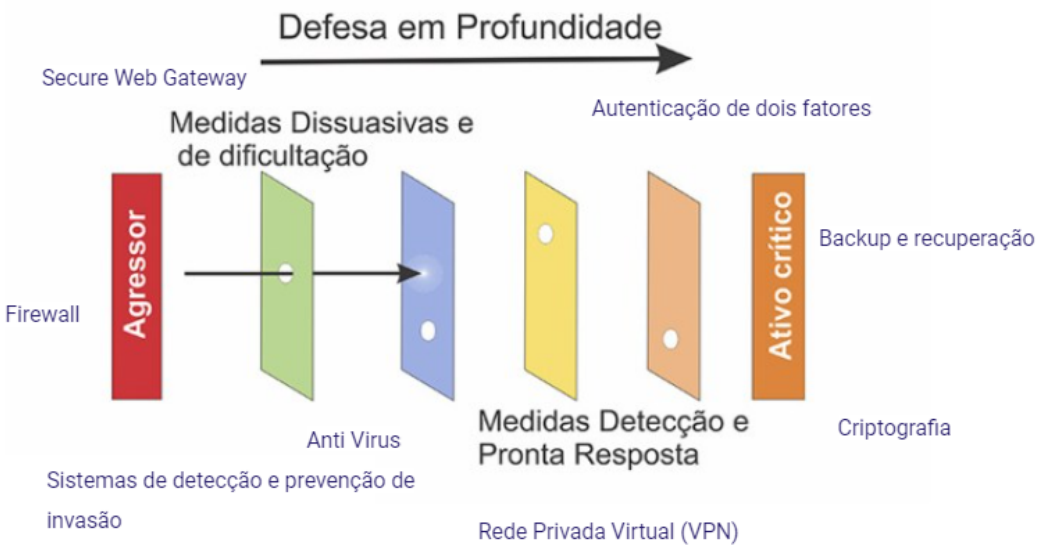
Fonte: Sêmola (2014, p. 49)

Analisando a figura, pode-se verificar a dimensão dos desafios na área de segurança da informação em ambientes sensíveis a dados pessoais.

À vista disso, ao implementar uma série de sistemas de defesa diferentes, como firewalls, antivírus, detecção de invasão, verificação de portas, gateways seguros, entre outros, podem ser cobertas as brechas que existiriam caso a rede dependesse somente de uma camada de segurança.

Neste processo, os componentes de segurança são dispostos em camadas, assim dificultando ataques. (NORTHCUTT et al., 2002)

Figura 4: Defesa em profundidade e seus elementos



Fonte: gestãodesegurancaprivada.com.br

Perímetros de Segurança

A segurança de perímetro é realizada por um firewall, capaz de filtrar todas as comunicações entre os servidores e dispositivos, que utiliza regras de segurança pré-definidas para permitir ou bloquear a passagem de dados. Alguns métodos que podem ser aplicados para a ferramenta Hestia são:

✓ Implantação de Firewall;
✓ Criptografia (discutido no item 7.1);
✓ Instalação de Rede Virtual Privada (VPN);
✓ Garantir conexão segura End to End;
✓ Garantir processo de autenticação;
✓ Limitar se não usar wifi.

6. Políticas de Segurança

Uma política de segurança é composta por regras que ditam o acesso, o controle e a transmissão da informação numa organização, a qual requer mudanças e atualizações constantes. Define o que é permitido e o que é proibido. A qual deve conter regras e diretrizes que orientem os colaboradores, e usuários com relação aos padrões de comportamento ligados à segurança da informação, condições de instalações de equipamentos, restrições de acesso, mecanismos de proteção, monitoramento e controle, entre outros cuidados imprescindíveis aos processos de negócio.

A Política de Segurança da Informação (PSI) trabalha com um conjunto de controles e mecanismos que garantem a integridade e segurança de uma estrutura de rede na qual exista o tráfego de informações e dados comuns e/ou restritos, e nela incluídos os equipamentos que armazenam tais informações. a política da segurança da informação, deve ser definida de acordo com a dificuldade de cada organização em manter suas informações seguras. O objetivo é preservar as informações quanto à integridade, confidencialidade e disponibilidade.

- Confidencialidade: Garante que o acesso à informação seja obtido, apenas, por pessoas autorizadas. A quebra desse sigilo pode acarretar danos inestimáveis para a empresa ou até mesmo para uma pessoa física;
- Integridade: Garante que a informação não seja adulterada falsificada ou furtada;
- Disponibilidade: Garante que a informação esteja disponível sempre que requisitada pelos usuários autorizados mesmo com as interrupções involuntárias de sistemas, ou seja, não intencionais.

Para o desenvolvimento da PSI são necessários treinamentos e cursos de capacitação para colaboradores que necessitam de um maior domínio sobre segurança da informação, como por exemplo os administradores de rede que têm que combater futuras tentativas de ataque e invasão. Assim como, a formação do termo de responsabilidade que tem a função de oficializar o acordo de que o colaborador tem o entendimento de suas obrigações de proteção das informações que manuseia.

Para a realização da PSI da ferramenta Hestia, deve ser considerada a aplicabilidade a todos os usuários, pessoa tutelar das informações, aos especialistas e pesquisadores do ramo e aos colaboradores de TI. Ela está baseada na norma NBR ISO/IEC 27.001.

Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais (Lei nº 9610).

É entendido que o sistema de segurança da informação somente será eficaz com o comprometimento de TODOS.

Comprometimento dos Usuários

- Respeitar esta Política de Segurança da Informação
- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional;
- Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc;
- Assegurar que as informações e dados de propriedade do paciente ou responsável não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico.
- Comprometer-se em não auxiliar terceiro ou não provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro.

Comprometimento dos Responsáveis Hierárquicos

- Apoiar e zelar pelo cumprimento desta **PSI**, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- Autorizar o acesso e definir o perfil do usuário junto ao gestor de liberação da área de TI,

- Autorizar as mudanças no perfil do usuário junto ao gestor de liberação da área de TI,
- Educar os usuários sobre os princípios e procedimentos de Segurança da Informação,
- Notificar imediatamente ao gestor de liberação da área de TI quaisquer vulnerabilidades e ameaças a quebra de segurança;
- Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

Comprometimento da Área de TI

- Configurar os equipamentos e sistemas para cumprir os requerimentos desta PSI,
- Restringir a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança do acesso público e manter evidências que permitam a rastreabilidade para auditoria ou investigação.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
- Administrar, proteger e testar as cópias de segurança dos programas e dados do negócio.
- Gerenciar o descarte de informações a pedido dos solicitantes.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários;
- Atribuir contas e senhas identificáveis a pessoa física para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação;
- Proteger todos os ativos de informação contra códigos maliciosos e ou vírus;
- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento;
- Realizar inspeções periódicas de configurações técnicas e análise de riscos;
- Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais;
- Garantir assim que solicitado o bloqueio de acesso de usuários por motivo de desligamento da instituição;
- Promover a conscientização dos colaboradores em relação a relevância da segurança da informação;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;
- Monitorar o ambiente de TI a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso a internet e aos sistemas críticos, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

O recomendável é a criação de uma metodologia formal, onde será definido como será realizada a manutenção, para que a mesma esteja sempre de acordo com as tecnologias que surgirem. Devem ser realizadas revisões sempre que novas ocorrências surgirem quanto estas acarretam impactos na segurança da informação da organização. Essas revisões devem englobar:

- Riscos imprevisíveis que forem identificados;
- Mudanças nas leis de negócios da organização;
- Eventuais falhas de segurança da informação;
- Fragilidades encontradas na segurança;
- Modificações na estrutura organizacional;
- Orientações do mercado a respeito de melhorias na segurança;

6.1. Permissões

Uma das maneiras de implementar uma política de controle de acesso é negar completamente os acessos aos usuários e, depois, permitir somente aqueles necessários para a execução de suas tarefas.

Essa autorização, preferencialmente, deve ser concedida e ser baseada no princípio da necessidade. Ou seja, apenas serão permitidos os recursos e permissões estritamente justificáveis para cada função.

Adotando essa estratégia, o sistema não corre o risco de deixar passarem despercebidas permissões inadequadas.

6.2 Regras de senha segura

Fornecer os acessos corretos será pouco efetivo caso seja permitido o uso de senhas fracas. Caso isso aconteça, um hacker ou mesmo um colaborador mal-intencionado, pode descobrir as credenciais de usuários com amplo acesso e, assim, roubar, apagar ou alterar informações.

Por isso, uma política de controle de acesso deve privilegiar a obrigatoriedade de boas práticas para criação. Alguns pontos que devem ser observados são a definição de um número mínimo de caracteres e o uso de letras maiúsculas e minúsculas, números e caracteres especiais.

Além disso, as senhas devem ser alteradas periodicamente e deve constar a proibição do uso de combinações repetidas dentro de um determinado período.

6.3 Auditoria

A movimentação de colaboradores dentro de uma organização pode acontecer com frequência. Mudanças de cargos, de setor, transferências, demissões etc. Todos esses acontecimentos precisam ser refletidos nas permissões dos usuários.

Logo, é importante que haja uma espécie de auditoria periódica para verificar se todos os usuários ativos permanecem na empresa. Além disso, é necessário avaliar se suas permissões de acesso estão de acordo com a vaga que estão ocupando.

6.4 Responsabilidades da área de TI

Organizar a logística de TI da organização, configurar os equipamentos, instalar softwares e implementar os controles necessários para cumprir os requerimentos de segurança estabelecidos pela

política de segurança da informação são fundamentais para que o documento elaborado tenha vida e funcionalidade na dinâmica da organização.

6.5 Política de treinamento aos colaboradores

Não basta implementar uma infinidade de sistemas de monitoramento de rede sem um correto treinamento dos usuários. É necessário, portanto, treinamento constante e conscientização de equipes, que podem ser previstos na política de segurança da informação.

7. Proposta para o Banco de Dados

Nesta seção, serão apresentadas as questões relativas aos bancos de dados para o sistema. As quais estão divididas em quatro seções: criptografia, controle de acesso e backup.

7.1 Criptografia

A criptografia é uma técnica bastante utilizada para proteger dados e informações que devem estar em sigilo, pois possuem valor em seu conteúdo. E por meio dela, é possível evitar que pessoas não autorizadas tenham acesso a esses dados armazenados, pois somente aquele que possui a devida chave de criptografia será capaz de visualizá-la.

A LGPD exige que medidas de segurança e salvaguardas sejam impostas, destaca a necessidade do uso de mecanismos técnicos e organizacionais adequados de segurança, como o uso de métodos de criptografia de banco de dados e iniciativas para o desenvolvimento seguro.

A seleção por um banco de dados adequado é um passo importante, por esta razão foi feita uma busca para coletar informações a seu respeito, para assim, ser feita uma seleção do melhor perfil. Seguindo os critérios: necessidades atuais do sistema, estimativa de acesso e projeção do crescimento dos dados, seguem os dados comparativos do estudo na Figura 5:

Figura 5: Bancos de Dados e suas Criptografias

Banco de Dados/ Criptografia	**Gerenciamento de chaves**	**TDE [1]**	**Always Encrypted**	**Criptografia de Backup**	**Oracle *Database Security***	**MD5 [2]**	**AES-256 [3]**	**CMK [4]**	**RBAC RCAC [5]**	**Auditoria**	**RMAN [6]**
Maria DB		x	x			x	x				
MySQL		x	x	x		x	x				
SQL Server Microsoft	x	x		x			x			x	
DB2 (IBM)							x		x		
Oracle					x					x	x
Amazon Aurora							x	x			

Fonte: Juliana Almeida Morroni (2020)

[1] TDE: Transparent Data Encryption - [2] MDS: Message-Digest algorithm 5 - [3] AES: Advanced Encryption Standard - [4] CMK: Client Master Key - [5] RBAC/RCAC: Controle de acesso baseado em função - [6] RMAN: Oracle Recovery Manager

O requisito para uma instalação de banco de dados segura é ter uma ferramenta de segurança como uma VPN (*Virtual Private Network*), que geralmente se utiliza de criptografia para deixar protegida toda a comunicação entre usuário e servidor.

Com base nisso, o próximo estudo foi baseado nos algoritmos de criptografia mais utilizados atualmente, para se obter um panorama de cada um, segue lista:

- Data Encryption Standard (DES) é uma das primeiras criptografias utilizadas e é considerada uma proteção básica de poucos bits. O seu algoritmo é o mais difundido mundialmente e realiza 16 ciclos de codificação para proteger uma informação.

- A criptografia 3DES recebe esse nome pelo fato de trabalhar com três chaves de 56 bits cada, o que gera uma chave com o total de 168 bits. O 3DES é uma cifragem da geração anterior que foi superada pelo aumento do poder de processamento.

- O Blowfish foi criado como alternativa à obsolescência do DES. É um dos primeiros algoritmos de cifragem de código aberto publicamente disponíveis. É conhecido por sua velocidade de encriptação e efetividade em geral. Trata-se de uma tecnologia bastante segura, pois há estudiosos no assunto que afirmam que o código não pode ser quebrado.

- O RC4 tem um principal benefício, sua velocidade; o algoritmo é muito rápido. Embora tenha algumas vulnerabilidades conhecidas, o RC4 pode ser útil quando é necessário segurança moderada.

- Padrão de Criptografia Avançada (AES) tornou-se um dos mais usados algoritmos de criptografia adotados pelos fabricantes de controle de segurança que contêm um componente de criptografia.

- Rivest, Shamir e Adleman (RSA) é o criptossistema de chave pública, atualmente considerado o padrão mais popular deste método. Ele é baseado no fato de ser muito difícil fatorar números grandes. Até agora, não há qualquer maneira conhecida de fazer isso rapidamente, e o RSA é considerado muito seguro para isto.

- Padrão de Assinatura Digital (DSS) é a assinatura usada pelo Governo dos Estados Unidos, que se baseia no Algoritmo de Assinatura Digital (DSA). Usada para gerar assinaturas digitais para autenticação de documentos eletrônicos.

- DES (Data Encryption Standard) = um dos modelos mais básicos e um dos primeiros a ser criado e implementado. Esse método pode ser decifrado por meio de uma técnica chamada "força bruta". Nesse caso, um programa testa, constantemente, todas as possibilidades de chave, de forma automatizada e por horas seguidas. Como é um sistema de proteção básica, oferece uma segurança reduzida para o usuário.

- IDEA (International Data Encryption Algorithm) = Ela atua de forma diferenciada, fazendo uma espécie de confusão para cifrar o texto, protegendo as informações e impedindo o realinhamento para a sua leitura de forma correta. Sua estrutura é bastante semelhante à do DES.

- AES (Advanced Encryption Standard) = É um dos algoritmos de criptografia mais seguros da atualidade, sendo utilizado até mesmo pelo Governo dos Estados Unidos. Sua criptografia é feita em blocos de 128 bits, mas as chaves podem ser aplicadas também em 192 e 256 bits, tornando essa chave extremamente difícil de ser quebrada em ataques convencionais de cibercriminosos.

Nesse sentido, tais criptografias e banco de dados estudados e avaliados neste trabalho serviram como base e apoio de possíveis recomendações futuras para o modelo de arquitetura da ferramenta Hestia que deve se fundamentar nos conceitos aqui abordados sobre privacidade de dados.

O Hestia em sua atual versão utiliza o SGBD (Sistema de Gerenciamento de Banco de Dados) um software para gestão de bases de dados, que permite criar, modificar e inserir elementos. O termo tem sua origem do inglês *Data Base Management System,* ou simplesmente DBMS. Ele é responsável por toda a gestão da base de dados. Ele salva informações, fornece os tópicos mais acessados, disponibiliza uma interface completa, controla o acesso à informação, entre muitas outras utilidades.
Entre alguns exemplos de SGBD no mercado, podem ser citados o SQL-Server, MySQL, SGBD Oracle entre outros, como mencionado na Figura 5.

7.2 Controle de Acesso

Uma vez que os requisitos de segurança da informação e os riscos possíveis sejam identificados, assim como o tratamento destes riscos tenha sido definido. Convém que controles pertinentes sejam selecionados e executados para assegurar a redução desses riscos a um nível aceitável.

Com referência à norma ABNT ISO/IEC 17799:2005, convém que todas as informações e ativos associados com os recursos de processamento da informação tenham um proprietário, designado por uma parte específica do sistema.

7.2.1 Proprietários dos ativos

Convém que o proprietário do ativo seja identificado e a ele seja atribuída a responsabilidade pela manutenção, conferência e alteração dos dados apropriada aos controles. A implementação de controles específicos pode ser delegada pelo proprietário, porém ele permanece encarregado pela proteção adequada dos dados. Ele, portanto, será responsável por:

- Assegurar que as informações e os ativos associados com os recursos de processamento da informação estejam adequadamente classificados;
- Definir e periodicamente analisar criticamente as classificações e restrições ao acesso, levando em conta as políticas de controle de acesso, aplicáveis.

O proprietário pode ser designado para: um processo, um conjunto de atividades definidas, uma aplicação ou um conjunto de dados.

Informação adicional: As tarefas de rotina podem ser delegadas, por exemplo, para um tutelar que cuida do ativo no dia-a-da, porém a responsabilidade permanece com o proprietário.

7.2.2 Inventário dos ativos

Convém que todas as informações incluindo, base de dados e arquivos, documentação de sistema, informações para pesquisa, procedimentos, histórico hospitalar, etc, sejam claramente identificados e um inventário seja estruturado e mantido, incluindo todas as informações importantes e necessárias que permitam a recuperação de dados.

7.2.3 Gerenciamento de usuários

Consiste na tarefa de realizar o controle e verificação de pessoas envolvidas e que interajam com o sistema (usuários), bem como o grupo de permissões de acesso aos recursos oferecidos, dispositivos, sistemas de armazenamento (banco de dados), redes, etc. Por se tratar de questões de confidencialidade (um dos pilares da LGPD), esse gerenciamento se torna algo fundamental e imprescindível.

Com esse gerenciamento, é permitido proporcionar maior eficiência, facilidade, rapidez e principalmente a segurança, garantindo que o sistema tenha um alto nível de controle do ambiente. O

nível de controle de acesso influencia diretamente na vulnerabilidade à brechas de segurança. Portanto quanto mais reforçado, mais difícil será a invasão do sistema. Os passos para se aplicar esse controle são:

- Processo de autenticação;
- Autorização;
- Auditoria.

O controle e gerenciamento dos usuários podem trazer diversos benefícios, tais como:

- Redução da complexidade;
- Hierarquia das permissões;
- Automatização e centralização da administração;

7.3 Backup

A importância do Backup está na proteção contra o risco de perda de dados e informações. Essa importância aumenta proporcionalmente em relação ao valor das informações a serem protegidas.

O Backup manual sempre oferece mais riscos, pois está sujeito a falhas humanas diversas, como esquecimento, armazenamento indevido ou até mesmo conhecimento técnico insuficiente. Além disso, toma muito tempo e reduz a produtividade operacional.

Por isso, as melhores práticas recomendam automatizar os Backups, de modo que ocorram de forma recorrente, respeitando as especificidades e regras do seu negócio.

Há diversas ferramentas ou softwares de automação Backup que são úteis no mercado, que oferecem, além da programação das cópias, a criptografia dos dados, dando maior transparência e segurança para confiar seus dados a um sistema.

7.3.1 Backup em Nuvem

Uma alternativa para atualizações seria o Backup em nuvem, que propõe a automatização das rotinas de cópias de segurança. Para utilizar este método, deve-se antes fazer um diagnóstico que aponte o espaço de armazenamento que será necessário, pois é isso que contratos em nuvem levam em conta.

Dependendo do sistema de backup utilizado, os dados serão automaticamente armazenados e protegidos na nuvem e poderão ser recuperados sempre que necessário.

8. Conclusões

Desde 2006, ano que o Hestia foi criado, houve mudanças significativas nas tecnologias de redes, bancos de dados e programação, assim como nos requisitos dos sistemas médicos e nas demandas legais, particularmente com as resoluções do Conselho Federal de Medicina e a Lei Geral de Proteção de Dados.

A arquitetura usada, a forte dependência de um SGBD específico são hoje consideradas limitações severas ao uso amplo do programa e à sua manutenção. A impossibilidade de utilizá-lo como SaaS ou de hospedá-lo diretamente em uma nuvem computacional tem reduzido o interesse de uso, licenciamento e evolução do software.

Portanto, é necessário um projeto completamente novo para o sistema, de forma a adaptá-lo às demandas atuais e futuras, incluindo a independência do SGBD, a portabilidade entre plataformas, o acesso remoto e o atendimento a exigências de segurança. Este último ponto é

bastante sensível, pois se trabalha com extensos registros de dados de crianças entre 0 e 2 anos, incluindo informações de caráter confidencial e médico das respectivas mães.

Este projeto deve contribuir para o desenvolvimento de um sistema distribuído de anamnese neurológica infantil de alto nível, com indicadores e campos de informação apropriados às características da população brasileira, próprio para uso em sistemas de saúde públicos e privados. A natureza distribuída prevista para o Hestia deverá habilitar a sua entrega como *Software as a Service*, incentivando organizações e empresas a assumirem as etapas de licenciamento, manutenção, evolução, distribuição, operação técnica e suporte ao programa, visto que estas responsabilidades são alheias aos objetivos da Universidade.

9. Referências

ABNT ISO 27002. (2013). ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR/ISO/IEC 27002:2013 tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação.

ADIL, Josué.Acadi-TI. **A importância do Backup para a segurança da informação no seu negócio.** Disponível em<https://acaditi.com.br/a-importancia-do-backup-para-a-seguranca-da-informacao-no-seu-negocio/#:~:text=O%20que%20%C3%A9%20Backup%3F&text=Considera%2Dse%20Backup%20qualquer%20c%C3%B3pia,acidentes%20operacionais%20com%20os%20equipamentos>. Acesso em 20 de maio de 2021.

ANGELIS, André F. **Projeto Hestia.** 2006 Disponível em:<https://sites.ft.unicamp.br/hestia/>. Acesso em: 06 de março de 2020.

Avast Software s.r.o. **O que é defesa em profundidade?** Disponível em:<https://www.avast.com/pt-br/business/resources/defense-in-depth>. Acesso em: 19 de maio de 2021.

BASTA, Alfred e BROWN, Mary. **Segurança de computadores e teste de invasão.** 2ª Edição. Local: Editora Cengage Do Brasil, 2014. p 173.

BRASIL. LEI nº 13.709, de 14 de agosto de 2018.

BRASIL. Resolução CFM nº 1.821/2007, de 23 de novembro de 2007.

BRASIL. Resolução CFM Nº 2.228, de 6 de fevereiro de 2019.

BRASIL. Resolução CFM nº 2.056/2013, de 12 de novembro de 2013.

BRAGANÇA, Carlos Eduardo Barbosa de Azevedo. **Segurança da Informação e privacidade de informações de pacientes de instituições de saúde: uma análise exploratória da privacidade percebida pelos profissionais HIPAA.** Disponível em:<https://www.bostonscientific.com/content/gwc/pt-BR/about-us/conformidade-e-etica/privacidade-dos-pacientes-e-hippa.html> Acesso em: 13 de novembro de 2020.

BS Brasil. **Perímetro de Segurança da Informação.** Disponível em:<https://www.mdrweb.com.br/bsbrasil/c.php?etp_id=PRO_03>. Acesso em 26 de junho de 2021.

CCM. **Segurança da informação: como fazer o controle de usuários?** Disponível em:<https://blog.ccmtecnologia.com.br/post/seguranca-da-informacao-como-fazer-controle-de-usuarios>. Acesso em: 02 de abril de 2021.

FJ REDEmpresa. **Política de Segurança da Informação.** Disponível em:<https://fj.com.br/politica-de-seguranca-da-informacao/>. Acesso em: 03 de maio de 2021.

Proof. **Como criar uma política de segurança da informação na sua empresa**. Disponível em:<https://www.proof.com.br/blog/politica-de-seguranca-da-informacao/> Acesso em: 05 de maio de 2021.

FREITAS, Cibelle. **Introdução à criptografia no MySQL.** Disponível em:< https://www.devmedia.com.br/introducao-a-criptografia-no-mysql/37179>. Acesso em: 12 de setembro de 2020.

GED - Gestão Eletrônica de Documentos (Portal ECM GED). Disponível em:< https://ged.net.br> Acesso em: 14 de outubro de 2020.

GUIMARÃES, Alexandre A. G. **Proposta de um modelo de segurança de VPNs na interligação de redes corporativas.** Tese (Mestrado em Engenharia Elétrica). Recife. Centro de Tecnologia e Geociências/Escola de Engenharia de Pernambuco, Universidade de Pernambuco.

MARQUES, Eduardo Pereira, et al. **Manual de Certificação para Sistemas de Registro Eletrônico em Saúde.** Disponível em:<http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2016_v4-2.pdf> Acesso em: 15 de outubro de 2020.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada.** Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018> Acesso em: 26 de setembro de 2020.

MOREIRA, Esdras. **ISO 27002: o que eu preciso saber?**
Disponível em:<https://introduceti.com.br/blog/iso-27002-o-que-eu-preciso-saber-descubra-aqui/>.Acesso em: 30 de maio de 2021.

NUNES, Natália Martins. **10 Princípios da LGPD.** Disponível em<https://ndmadvogados.jusbrasil.com.br/artigos/698194397/10-principios-da-lgpd-para-o-tratamento-de-dados-pessoais> Acesso em: 31 de março de 2021.

RIBEIRO, Cristiano da Silva. **Segurança da Informação**: o desenvolvimento de uma política de segurança da informação em conformidade com a norma ABNT *ISO/IEC* 27002. Ano 2016. 35 páginas. Trabalho de Conclusão de Curso de Sistema de Informação – FAIR Faculdades Integradas de Rondonópolis, 2016.

SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva - 2 ed**. São Paulo: Elsevier, 2014.

SERPRO. **O que são dados sensíveis, de acordo com a LGPD**. Disponível em: <https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd> Acesso em: 26 de setembro de 2020.

S. ROCHA, Yan; LIMA, Eliomar A. de. **Aplicabilidade da Norma ABNT NBR ISO/IEC 27002 em uma Empresa de Médio Porte. In: Escola regional de informática de Goiás (ERI-GO)**, 2018. , 2018, Goiânia. Anais da VI Escola Regional de Informática de Goiás. Porto Alegre: Sociedade Brasileira de Computação, aug. 2018 . p. 273-282.

SYDLE. **GED: Como funciona o Gerenciamento Eletrônico de Documentos? Disponível em:<**https://www.sydle.com/br/blog/ged-como-funciona-5f58df091e43744c69b51502/>. Acesso em: 30 de janeiro de 2020.

SYNNEX Corporation. **O Que É Segurança De Perímetro E Como Ela É Afetada Pela Cloud Computing?** Disponível em:< https://blogbrasil.comstor.com/o-que-seguranca-de-perimetro-e-como-ela-afetada-pela-cloud-computing> Acesso em: 22 de abril de 2021.

Valid Certificadora(6 de fevereiro de 2019). **Tipos de criptografia: conheça os 10 mais usados e como funciona cada um – Ouça.** Disponível em:<https://cryptoid.com.br/valid/tipos-de-criptografia-conheca-os-10-mais-usados-e-como-funciona-cada-um/>.

William Stallings. 2007. Criptografia e Segurança de Redes: Princípios e Práticas – 4ª Edição.

DocuSign**. Política de segurança da informação: saiba como e por que desenvolvê-la.** Disponível em:<https://www.docusign.com.br/blog/politica-de-seguranca-da-informacao-saiba-como-e-por-que-desenvolve-la>. Acesso em: 03 de maio de 2021.

Outras fontes consultadas

http://certforum.iti.gov.br/2015/brasilia/wp-content/uploads/2014/10/apresentacao_marcelo_silva.pdf
http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2016_v4-2.pdf
https://aws.amazon.com/pt/compliance/hipaa-compliance/
https://blog.imedicina.com.br/seguranca-de-softwares-medicos-tudo-o-que-voce-precisa-saber/
https://cmtecnologia.com.br/blog/garantir-seguranca-informacao/

https://portal.cfm.org.br/images/PDF/resolucao222718.pdf

https://www.crasp.gov.br/centro/conteudo/old/uploads/Eliminacao_do_papel_na_area_da_Saude_certificacao_SBISCFM_ANS.pdf
https://www.iti.gov.br/noticias-iti/2496-certificado-icp-brasil-sera-requisito-de-seguranca-no-atendimento-medico-a-distancia
https://www.pixeon.com/blog/praticas-essenciais-para-seguranca-da-informacao-na-area-da-saude/
https://www.secad.com.br/blog/medicina/como-garantir-seguranca-de-dados-consultorio/